A general method to implement an arbitrary unitary operator in quantum computation

Jaehyun Kim, J. S. Lee, and Soonchil Lee

Department of Physics, Korea Advanced Institute of Science and Technology, Taejon, 305-701, Korea

(August 17, 1999)

It has been proved that an arbitrary unitary operation can be performed by a quantum computer but a general implementation procedure is not known yet. We present a general method which expresses an unitary operator by the product of operators allowed by Hamiltonians. In this method, the generator of an operator is found first, and then the generator is expanded by the base operators of the product operator formalism. Finally, the base operators disallowed by the Hamiltonian of a quantum computer, including more than 2-body interaction operators, are substituted with allowed ones by the axes transformation and coupling order reduction technique.

In 1973, Bennett proposed a reversible Turing machine which is as efficient as an irreversible one [1] and this led to the idea of using quantum system as a computer because the time evolution of a quantum system is reversible. Feynman introduced a concept of a quantum computer [2] and its theoretical model was given by Deutsch [3]. On the other hand, Fredkin and Toffoli proved that an arbitrary computation can be performed by a reversible Turing machine by showing that AND, OR and NOT gates can be generated by reversible 3-bit gates [4] among which a Toffoli gate is most frequently used now a days [5]. In quantum computation, a 3-bit gate cannot be implemented directly because it requires a simultaneous interaction of three particles. Thus, there have been efforts to find 2-bit universal gates [6–12]. Especially, Barenco *et al.* showed that a combination of 2-bit C-NOT gates and 1-bit gates can replace a Toffoli gate and proposed a method to make general n-bit controlled gates [13]. Therefore, it is proved that an arbitrary computation can be performed by a quantum computer and the implementation of these universal gates became the basic requirement for any quantum system to be a quantum computer.

However, the proof that an arbitrary computation can be done by a quantum computer does not necessarily mean that we know a general implementation procedure. If an unitary operator U, equivalent to a combination of gates, is related to a Hamiltonian $\mathcal{H}$ of a certain quantum system by $U = \exp(-\imath\mathcal{H}t/\hbar)$, it can be realized by the time evolution of the system during time t. But there are only a few operations which can be implemented in this way by the limited Hamiltonians of nature. Therefore, it is very necessary to find a general method to implement an arbitrary operation using only the given Hamiltonians. Feynman proposed a way to construct an artificial Hamiltonian when U is given by $U = U_k \cdots U_3U_2U_1$ and all $\mathcal{H}_i$'s corresponding to U_i's exist in nature [14], but it is impractical to construct artificial Hamiltonians. It will be more practical to partially control a Hamiltonian by turning "on" and "off" perturbations if U can be expressed as a product of operators corresponding to the perturbation terms. Whether Feynman's artificial Hamiltonians or switch-able perturbations are used, an operator of interest should be expressed as a product of the operators allowed by Hamiltonians. This is equivalent to finding the combination of universal gates and generally very difficult problem having several solutions.

In this work, we propose a general method of expressing any unitary operator as a product of operators allowed by nature. This method makes use of the fact that an unitary operator U is always given by $U = \exp[-\imath G]$, where G is a Hermitian operator. Once the generator of an operator, G, is found, it is expanded by suitable base operators. Then U is expressed as a product of operators having only one base operator as a generator and, finally, each operator in the product is replaced by the allowed ones.

The first step of implementation is to find the generator of a given operator. Since the only way to implement an operator is to use the time evolution of a state under a suitable Hamiltonian, a generator, which is a product of Hamiltonian and time, gives physical information necessary for implementation. An unitary operator is represented by a normal matrix and always diagonalized by unitary transformation. The matrix T which diagonalizes U also diagonalizes G as

$$U' = TUT^\dagger = e^{-\imath TGT^\dagger} = e^{-\imath G'}, \qquad (1)$$

where U' and G' are diagonalized matrices of U and G, respectively. Once the operator and its generator become diagonal, G' is easily obtained from

$$U'_{kk} = e^{-\imath G'_{kk}} \qquad (2)$$

and G is obtained by inverse transformation $G = T^\dagger G' T$. Since G is Hermitian, the eigenvalues of G, G'_{kk}, are real and U'_{kk} are complex with absolute value of unity. It is worthwhile to note that the mapping from U'_{kk} to G'_{kk} is not unique.

To relate the generator G with Hamiltonians, consider the following operators of the product operator formalism for N spin-$\frac{1}{2}$ particles [15–17].

$$B_s = 2^{(q-1)}(I_{\alpha_1} \otimes I_{\alpha_2} \otimes \cdots \otimes I_{\alpha_N}), \tag{3}$$

where $s = \{\alpha_1, \alpha_2, \cdots, \alpha_N\}$ and α_i is 0, x, y, or z. I_0 is E, i.e., a 2×2 unity matrix, I_{α_i} is a spin angular momentum operator for $\alpha_i \neq 0$, and q is the number of nonzero α_i's. For example, $\{B_s\}$ for $N = 2$ is given by

$$\begin{array}{ll} q = 0 \;\; ; & E/2 \\ q = 1 \;\; ; & I_{1x}, I_{1y}, I_{1z}, I_{2x}, I_{2y}, I_{2z} \\ q = 2 \;\; ; & 2I_{1x}I_{2x}, 2I_{1x}I_{2y}, 2I_{1x}I_{2z}, \cdots, \end{array} \tag{4}$$

which are 16 Dirac matrices except the factor of $\frac{1}{2}$. In Eq. 4, unity matrices are not shown and spin index is added for convenience. $\{B_s\}$, consisting of 4^N elements, makes a complete set and therefore, an arbitrary $2^N \times 2^N$ matrix can be expanded by the linear combination of B_s's. Since G and B_s's are Hermitian, coefficients of the linear expansion are real numbers and obtained by applying the inner product of G and B_s's.

An unitary operator is now expressed as $U = \exp(-\imath \sum_s b_s B_s)$ of which the generator is related to physical observables. In general, there exists no Hamiltonian which corresponds to a linear combination of B_s's. Therefore, our next step is to express U as a product of *single operators* which have only one B_s as a generator like $\exp[-\imath b_s B_s]$. Sometimes, this decomposition is the most difficult step and it is not proved yet whether the decomposition is generally possible even for spin operators. Fortunately, many useful gates can be easily decomposed by using the commutation relations of B_s's. B_s's are either commuting or anticommuting each other. If G is expanded with only commuting B_s's, U can be easily represented by a product of single operators as

$$U = \exp[-\imath \sum_s b_s B_s] \rightarrow \prod_s \exp[-\imath b_s B_s]. \tag{5}$$

A swap gate and an f-controlled phase shift gate used in Grover's search algorithm belong to this case.

Even though a generator has non-commuting B_s's, there are cases where decomposition is straightforward. Suppose two base operators, B_{s1} and B_{s2}, satisfy the relation ($\hbar = 1$),

$$[B_{s1}, B_{s2}] = \imath B_{s3}, \tag{6}$$

then B_{s3} also belongs to $\{B_s\}$. This commutation relation makes the three operators, B_{s1}, B_{s2}, and B_{s3}, transform like Cartesian coordinates under rotation, meaning that

$$\exp[-\imath\phi B_{s3}] B_{s1} (\exp[-\imath\phi B_{s3}])^\dagger = B_{s1}\cos\phi + B_{s2}\sin\phi, \tag{7}$$

for cyclic permutations of $s1$, $s2$, and $s3$. If a generator has only these operators, it can be decomposed using Euler rotations. For example, $\exp[-\imath\phi(B_{s1} + B_{s2})]$ is understood to be the rotation with the angle of $\sqrt{2}\phi$ about the axis 45° off the "B_{s1}-axis" on the plane of B_{s1} and B_{s2} axes. Therefore, this operation is equivalent to the successive rotations about B_{s1} and B_{s3} axes as follows,

$$e^{-\imath\phi(B_{s1}+B_{s2})} = e^{-\imath\frac{\pi}{4}B_{s3}} e^{-\imath\sqrt{2}\phi B_{s1}} e^{\imath\frac{\pi}{4}B_{s3}}. \tag{8}$$

This decomposition technique by Euler rotations is also applicable when an operator has a generator in the factorized form as follows,

$$U = \exp\left[-\imath \prod_{i=1}^{N} (\sum_{\alpha_i} \phi_{i\alpha_i} I_{i\alpha_i})\right], \tag{9}$$

where $\phi_{i\alpha_i}$ are real numbers. Since I_{1x}, I_{1y}, and I_{1z} satisfy the commutation relation in Eq. 6, and commute with any other spin operators with $i \neq 1$, spin 1 components are decomposed as,

$$U_1 \exp\left[-\imath(\phi_{10}E + \phi_1 I_{1\alpha_1}) \prod_{i=2}^{N} (\sum_{\alpha_i} \phi_{i\alpha_i} I_{i\alpha_i})\right] U_1^\dagger, \tag{10}$$

where U_1 is the product of the single operators of which the generators have only spin 1 components, corresponding to Euler rotations. Repeated applications of this process to successive spins give

$$U = U_N \cdots U_1 e^{-\imath G} U_1^\dagger \cdots U_N^\dagger, \tag{11}$$

where

$$G = \prod_{i=1}^{N} (\phi_{i0}E + \phi_i I_{i\alpha_i}). \tag{12}$$

Then, decomposition is finished because all terms in Eq. 12 commute each other. All the controlled gates belong to this case. If none of the above methods are applicable, U can be approximately expanded as a product of single operators to any desired accuracy [18].

Although B_s is a product of spin operators which are physical quantities, not all B_s's exist in Hamiltonians that nature allows. Our final step of implementation is to substitute disallowed single operators in the product with allowed ones. The Hamiltonian of a real quantum system used for implementation of a quantum computer allows only the following single operators in general.

$$\begin{array}{l} R_{i\alpha}(\phi) = e^{-\imath\phi I_{i\alpha}}, \\ J_{ij\alpha}(\phi) = e^{-\imath\phi 2 I_{i\alpha} I_{j\alpha}}. \end{array} \tag{13}$$

The first term is a rotation operator which rotates spin i about α-axis by the angle of ϕ and the second one is a spin-spin interaction operator between spins i and j. The angle ϕ in the second term is proportional to the spin-spin coupling constant and evolution time, but we denote it as a rotation angle because the effect of spin-spin interaction can be understood as a rotation of one spin due to the magnetic field of the other. Before going further, we assume the following more restricted set of operators as allowed ones in this study.

$$\begin{aligned} R_{i\alpha}(\phi) &= e^{-\imath\phi I_{i\alpha}} \quad (\alpha = x \text{ or } y), \\ J_{ij}(\phi) &= J_{ijz}(\phi) = e^{-\imath\phi 2I_{iz}I_{jz}}. \end{aligned} \tag{14}$$

In this set, only x and y axes are used for single spin rotations and a spin-spin interaction is limited to the Ising type. Needless to say, the more single operators are allowed, the easier it is to implement an algorithm. However, Eq. 14 is an enough set to realize any unitary operators as shown below and in fact these are the only operators allowed by an NMR quantum computer, which has been the most successful quantum computer so far. Two rotation operators can generate any single bit operation and the interaction operator can make a c-NOT gate in combination with rotation operators [19,20]. Therefore, these three operators consist the minimum set to implement universal gates. Though they are the operators allowed in the quantum computers using spin-$\frac{1}{2}$ particles as qubits, corresponding operators must be allowed to realize universal gates in any implementations. Therefore, we can safely assume that Eq. 14 is the set of generally allowed operators without loss of generality.

Now, we are to show that the minimum set in Eq. 14 can generate all the other operators of $\{B_s\}$. First, the single bit operation excluded in Eq. 14, $R_{iz}(\phi)$, can be transformed from $R_{ix(y)}(\phi)$ as

$$R_{iz}(\phi) = R_{iy(x)}(-\frac{\pi}{2})R_{ix(y)}(\phi)R_{iy(x)}(\frac{\pi}{2}). \tag{15}$$

This is the composite pulse technique well-known in NMR experiment [16]. Any rotation about one axis can be replaced by the composite of rotations about the other two. This technique can be immediately applied to transform an n-th order operator meaning the single operator which has a generator B_s with $q = n$. All the second order operators can be transformed to the Ising type operator in Eq. 14 by this composite pulse technique. For example, $U(\phi) = \exp[-\imath\phi 2I_{ix}I_{jz}]$ is transformed as [21]

$$\begin{aligned} \exp[-\imath\phi 2I_{ix}I_{jz}] &= \exp[-\imath\phi R_{iy}(\tfrac{\pi}{2})(2I_{iz}I_{jz})R_{iy}(-\tfrac{\pi}{2})] \\ &= R_{iy}(\tfrac{\pi}{2})\exp[-\imath\phi 2I_{iz}I_{jz}]R_{iy}(-\tfrac{\pi}{2}). \end{aligned} \tag{16}$$

The operators with more than 2-body interaction can be reduced to the Ising type 2-body interaction operator as discussed below after all the spin coordinates are changed to z using this technique. From now on, we call the n-body interaction operators with all $\alpha_i = z$ the n-th order coupling operator. The key idea of the coupling order reduction is that the n-th order coupling can be thought as the $(n-1)$-th order coupling controlled by one spin state. For example, the third order coupling operator, $\exp[-\imath\phi 4I_{iz}I_{jz}I_{kz}]$, is represented by

$$\begin{aligned} &\exp[-\imath\phi 4I_{iz}I_{jz}I_{kz}] \\ &= \exp\left[-\imath\phi\begin{pmatrix} 2(I_z\otimes I_z) & 0 \\ 0 & -2(I_z\otimes I_z)\end{pmatrix}\right] \\ &= \begin{pmatrix} \exp[-\imath\phi 2(I_z\otimes I_z)] & 0 \\ 0 & \exp[\imath\phi 2(I_z\otimes I_z)]\end{pmatrix} \\ &= \begin{pmatrix} J_{jk}(\phi) & 0 \\ 0 & J_{jk}(-\phi)\end{pmatrix} \end{aligned} \tag{17}$$

in the subspace of spin i. The final form of Eq. 17 implies that the third order coupling operator can be understood as the second order one with the coupling between spin j and k but its rotation direction depends on the state of spin i. We note that if one spin is flipped during the evolution of a spin-spin interaction, then the sign of interaction changes and this has effect of time reversal. This means that the rotation direction changes [16,20], and therefore, we can implement Eq. 17 with the second order coupling operator by flipping spin j or k depending on the state of spin i. It is a well-known c-NOT(XOR) gate which flips one spin depending on the state of the other spin. A c-NOT gate is given by

$$\begin{aligned} U_{\text{c-NOT}} &= R_{iz}(\tfrac{\pi}{2})R_{jx}(\tfrac{\pi}{2})R_{jy}(\tfrac{\pi}{2})J_{ij}(-\tfrac{\pi}{2})R_{jy}(-\tfrac{\pi}{2}) \\ &= R_{iz}(\tfrac{\pi}{2})U_{ij} \end{aligned} \tag{18}$$

up to overall phase and this is a product of allowed operators in Eq. 14. In the same way, the n-th order coupling operator can be reduced to the $(n-1)$-th order one by conditionally flipping odd number of spins except the spin i. Repeated applications of this process obviously reduce the n-th order coupling operator to the second order one. Fig. 1 shows the quantum networks of the n-th order coupling operator and its equivalent combination of the allowed operators. In Fig. 1 (b), c-NOT gates after the second order coupling operator are inserted to flip spins to their original states. Instead of c-NOT gates before and after the second order coupling operator, U_{ij} and $U_{ij}^\dagger$ can be used either, respectively.

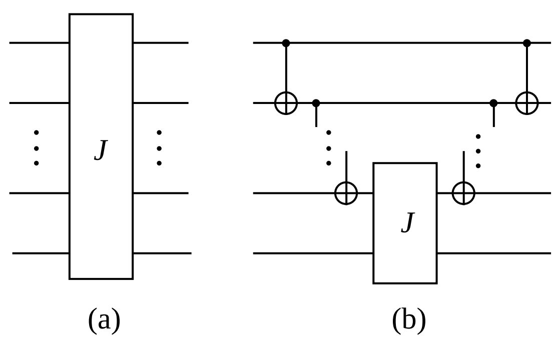

FIG. 1. Quantum network for the n-th order coupling operator (a) and its equivalent network consisting of allowed operators (b).

As an example, we apply this general implementation procedure to a Toffoli gate. The generator of a Toffoli gate obtained after the process of diagonalization and inverse unitary transformation is expanded by base operators as

$$\begin{aligned} G = \pi(& -\tfrac{1}{8}E + \tfrac{1}{4}I_{1z} + \tfrac{1}{4}I_{2z} - \tfrac{1}{4}2I_{1z}I_{2z} + \tfrac{1}{4}I_{3x} \\ & - \tfrac{1}{4}2I_{1z}I_{3x} - \tfrac{1}{4}2I_{2z}I_{3x} + \tfrac{1}{4}4I_{1z}I_{2z}I_{3x}). \end{aligned} \tag{19}$$

Since all terms in this generator commute each other, the corresponding operator is easily expressed as a product of single operators. After substituting disallowed operators, $I_{1z}I_{3x}$ and $I_{1z}I_{2z}I_{3x}$ in this case, with allowed ones by the axes transformation and order reduction, the gate is finally expressed as

$$\begin{aligned} & R_{1z}(\tfrac{\pi}{4})R_{2z}(\tfrac{\pi}{4})J_{12}(-\tfrac{\pi}{4})R_{3x}(\tfrac{\pi}{4})R_{3y}(\tfrac{\pi}{2})J_{13}(-\tfrac{\pi}{4}) \\ & \times J_{23}(-\tfrac{\pi}{4})U_{12}J_{23}(\tfrac{\pi}{4})U_{12}^{\dagger}R_{3y}(-\tfrac{\pi}{2}), \end{aligned} \tag{20}$$

up to overall phase.

In summary, we propose a general method to implement an arbitrary unitary operator using generator expansion. Since generators are closely related with Hamiltonians, they help to see the physical meaning of an operation. The operators with generators disallowed by Hamiltonians are replaced by allowed ones using the axes transformation and order reduction technique. Therefore, our method also makes it possible to simulate an Hamiltonian which does not exist in nature, including more than 2-body interactions. In the future, a compiler which translates a unitary operator into the product of allowed ones automatically should be developed to make a practical quantum computer. Our method necessarily gives neither optimal nor unique solution to implementation as the mapping from U'_{kk} to G'_{kk} in Eq. 2 is not unique. It is an open question yet which choice would give an optimal solution.

[1] C. H. Bennett, IBM J. Res. Dev. **6**, 525 (1973).

[2] R. P. Feynman, Int. J. Theor. Phys. **21**, 467 (1982).

[3] D. Deutsch, Proc. R. Soc. Lond. A **400**, 97 (1985).

[4] Fredkin and T. Toffoli, Int. J. Theor. Phys. **21** 219 (1982).

[5] T. Toffoli, in *Automata, Languages and Programming*, edited by J. W. de Bakker and J. van Leeuwen (Spinger, New York, 1980).

[6] D. Deutsch, Proc. R. Soc. Lond. A **425**, 73 (1989).

[7] D. P. DiVincenzo, Phys. Rev. A **51**, 1015 (1995).

[8] D. Deutsch, A. Barenco, and A. Ekert, Proc. R. Soc. Lond. A **449**, 669 (1995).

[9] A. Barenco, Proc. R. Soc. Lond. A **449**, 678 (1995).

[10] S. Lloyd, Phys. Rev. Lett. **75**, 346 (1995).

[11] A. Barenco, D. Deutsch, A. Ekert, and R. Jozsa, Phys. Rev. Lett. **74**, 4083 (1995).

[12] T. Sleator and H. Weinfurter, Phys. Rev. Lett. **74**, 4087 (1995).

[13] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).

[14] R. P. Feynman, *Feynman Lectures on Computation*, edited by A. J. G. Hey and R. W. Allen (Addison-Wesley, New York, 1996).

[15] O. W. Sörensen, G. W. Eich, M. H. Levitt, G. Bodenhausen, and E. Ernst, Prog. NMR Spect. **16**, 163 (1983).

[16] E. Ernst, G. Bodenhausen, and A. Wokaun, *Principles of Nuclear Magnetic Resonance in One and Two Dimensions* (Oxford Univ. Press, Oxford, 1987).

[17] S. S. Somaroo, D. G. Cory, and T. F. Havel, Phys. Lett. A **240**, 1 (1998)

[18] A. T. Sornborger and E. D. Stewart, quant-ph/9903055 (1999).

[19] J. Jones, R. H. Hansen, and M. Mosca, J. Magn. Res. **135**, 353 (1998).

[20] N. Linden, H. Barjat, R. J. Carbajo, and R. Freeman, quant-ph/9811043 (1998).

[21] T. F. Havel, S. S. Somaroo, C.-H. Tseng, and D. G. Cory, quant-ph/9812086 (1998).